

► KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Controles de terminales

Las potentes herramientas de control de terminales perfectamente integradas con programas antimalware de vanguardia y el único laboratorio de Lista blanca dedicado del sector, permiten proteger su negocio del dinámico ambiente de las amenazas actual.

PROTEGER, HACER VALER, CONTROLAR

Las vulnerabilidades en las aplicaciones de confianza, el malware basado en la web y la falta de control sobre los dispositivos periféricos forman parte de un paisaje de amenazas cada vez más complejo. La aplicación y las herramientas web y de control de dispositivos de Kaspersky Lab, le brindan un control absoluto de los terminales sin comprometer la productividad.

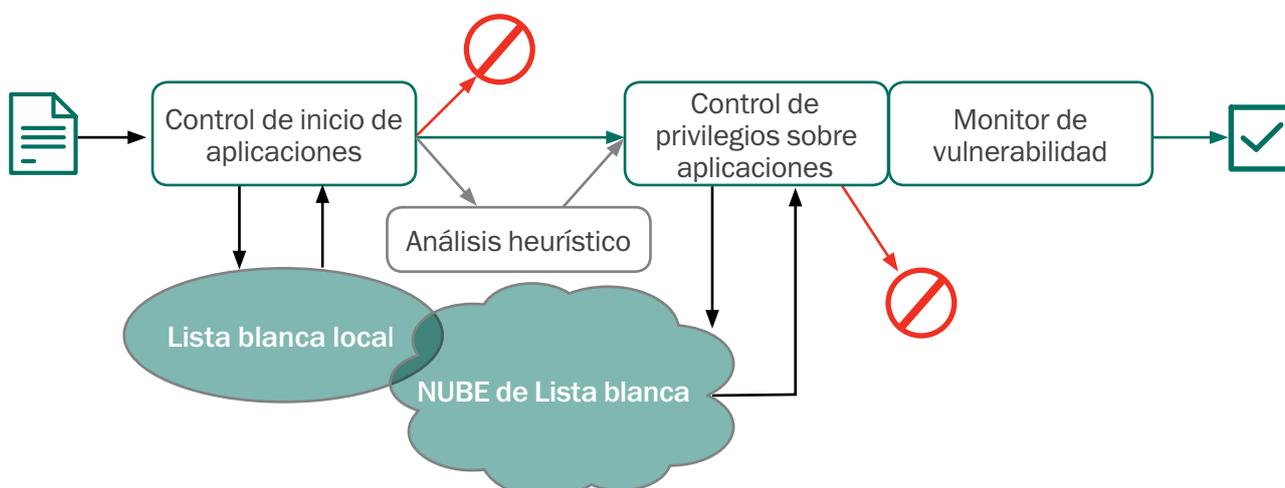
CONTROL DE APLICACIONES Y LISTA BLANCA DINÁMICA

Protege los sistemas de las amenazas conocidas y desconocidas, por lo que ofrece a los administradores control total sobre las aplicaciones y los programas que se pueden ejecutar en los terminales, independientemente del comportamiento de los usuarios finales. Además, permite la supervisión de integridad de las aplicaciones para evaluar su comportamiento y evitar la ejecución de acciones inesperadas que podrían poner en peligro el terminal o la red. En palabras simples, la creación y aplicación personalizable o automatizada de políticas permite:

- **Control del inicio de las aplicaciones:** permitir, bloquear, auditar la ejecución de las aplicaciones. Impulsar la productividad mediante la restricción de acceso a aplicaciones no empresariales.
- **Control de privilegios de la aplicación:** regular y controlar el acceso de la aplicación a los recursos y datos del sistema. Clasificar las aplicaciones como de confianza, no de confianza o restringidas. Administrar el acceso de las aplicaciones a los datos cifrados en los terminales, como la información publicada a través de navegadores web o Skype.
- **Escaneo de vulnerabilidades de aplicaciones:** defensa proactiva contra los ataques dirigidos a las vulnerabilidades en las aplicaciones de confianza.

La mayoría de las soluciones de control solo ofrecen funcionalidades básicas de bloqueo/acceso. Las herramientas de control de Kaspersky Lab son únicas en su uso de bases de datos de listas blancas basadas en la nube, lo que les permite un acceso casi en tiempo real a los datos más recientes de las aplicaciones.

Las tecnologías de control de aplicaciones de Kaspersky Lab usan bases de datos de listas blancas basadas en la nube para analizar y controlar las aplicaciones en cada una de las etapas: descarga, instalación y ejecución.



Las listas blancas dinámicas, que se pueden activar a través de una completa "negación predeterminada", bloquean todas las aplicaciones que intentan ejecutarse en cualquier estación de trabajo, a menos que los administradores las permitan explícitamente. Kaspersky Lab es la única empresa de seguridad con un laboratorio de Lista blanca dedicado, que mantiene una vigilancia constante y cuenta con una base de datos actualizada con más de 500 millones de programas.

La negación predeterminada de Kaspersky Lab **se puede aplicar en un entorno de prueba**, lo que les permite a los administradores establecer la legitimidad de una aplicación antes de bloquearla. Además, se pueden crear categorías de aplicaciones basadas en firmas digitales, evitando que los usuarios ejecuten software legítimo modificado por malware o que proviene de una fuente sospechosa.

CONTROLES WEB

Monitoree, filtre y controle los sitios web a los que los usuarios pueden acceder en el lugar de trabajo, aumentando la productividad a la vez que se protege contra el malware basado en la web y los ataques.

Los controles web avanzados de Kaspersky Lab se basan en un directorio en constante actualización de sitios web, que se agrupan en categorías (p. ej., para adultos, juegos, redes sociales, juegos de azar). Los administradores pueden crear fácilmente políticas para prohibir, limitar o auditar la utilización de cualquier sitio individual o categorías de sitio por parte del usuario final, así como crear sus propias listas. Los sitios malintencionados se bloquean automáticamente.

Y gracias a que restringe su uso, el control web de Kaspersky Lab permite evitar la pérdida de datos a través de servicios en redes sociales y de mensajería instantánea. Las políticas flexibles permiten a los administradores permitir la navegación a determinadas horas del día. Y la integración con Active Directory significa que se pueden aplicar políticas en toda la organización de forma rápida y sencilla.

Para mayor seguridad, los controles web de Kaspersky Lab se habilitan directamente en el terminal, lo que significa que las políticas se aplican incluso cuando el usuario no está en la red.

CONTROLES DEL DISPOSITIVO

Desactivar un puerto USB no siempre resuelve sus problemas con los dispositivos extraíbles. Por ejemplo, un puerto USB desactivado impacta sobre otras medidas de seguridad, como por ejemplo, los VPN con token de acceso.

El control de dispositivos de Kaspersky Lab permite un nivel más granular de control a nivel del bus, tipo y dispositivo, con lo cual se mantiene la productividad del usuario final al mismo tiempo que se optimiza la seguridad. Se pueden aplicar controles hasta del número de serie específico del dispositivo.

- También establecer permisos de conexión/lectura/escritura para los dispositivos, así como planificación de tiempo.
- Crear reglas de control de dispositivos basadas en máscaras, eliminando la necesidad de conectar físicamente los dispositivos para agregarlos a la lista blanca. Agregar varios dispositivos a la Lista blanca simultáneamente.
- Intercambiar datos a través de dispositivos extraíbles, dentro y fuera de la organización, y reducir el riesgo de pérdida o robo de datos.
- Integrar las tecnologías de cifrado de Kaspersky Lab para hacer cumplir las políticas de cifrado sobre tipos específicos de dispositivo.

FÁCIL ADMINISTRACIÓN

Todas las herramientas de control de Kaspersky Lab se integran con Active Directory, por lo que la configuración general de políticas es simple y rápida. Todos los controles de terminales se administran desde la misma consola, a través de una sola interfaz.

Cómo comprar

Las herramientas de control de terminales de Kaspersky Lab no se venden por separado. Están habilitadas en los niveles "Select", "Advanced" y "Total" de Kaspersky Endpoint Security for Business.